WE CLAIM:

1. An apparatus for managing access to a resource over a network, comprising:

a receiver arranged to receive a request for access to the resource from a client device; and

a policy manager, coupled to the receiver, that is arranged to perform actions, including:

determining a configuration of the client device;

applying a dynamic policy for the access based, in part, on the determined configuration; and

applying a restriction to the access for the requested resource based on the applied dynamic policy.

2. The apparatus of claim 1, wherein determining the configuration of the client device further comprises:

if the client device is configured to receive a downloadable component, providing the downloadable component to the client device.

3. The apparatus of claim 2, wherein the downloadable component is configured to inspect an environment of the client device and provide environment information to the policy manager.

4. The apparatus of claim 1, wherein determining the configuration of the client device further comprises determining information associated with the connection between the client device and the resource.

5. The apparatus of claim 1, further comprising in response to receiving the request for access to the resource, transmitting a downloadable component to the client device.

6. The apparatus of claim 1, wherein applying the restriction further comprises employing a virtual sandbox that is configured based on the applied dynamic policy.

7. The apparatus of claim 1, wherein the restriction includes at least one downloadable component.

8. The apparatus of claim 1, wherein the restriction is configured to intercept a communication between the client device and the apparatus.

9. The apparatus of claim 1, wherein applying the restriction further comprises performing at least one of intercepting a system command, inhibiting a file save, inhibiting a file print, restricting launching of a predetermined application, and redirecting access to a file.

10. A method of managing access to a resource over a network, comprising:

receiving a request for access to the resource from a client device;

determining a configuration of the client device;

applying a dynamic policy for the access based, in part, on the determined configuration; and

applying a restriction to the access for the requested resource based on the applied dynamic policy.

11. The method of claim 10, further comprising in response to receiving the request for access to the resource, transmitting a downloadable component to the client device.

12. The method of claim 10, wherein determining the configuration further comprises,

if the client device is configured to receive a downloadable component, providing the downloadable component to the client device, wherein the downloadable component is configured, in part, to determine the configuration of the client device.

13. The method of claim 10, wherein determining the configuration further comprises determining at least one of one level of trust associated with the client device, a type of encryption enabled on the client device, a type of antivirus enabled on the client device, a security feature enabled on the client device, a browser type, an operating system configuration, a security certificate, and if a hacker tool is enabled on the client device.

14. The method of claim 10, wherein determining the configuration further comprises determining a level of trust of the client device.

15. The method of claim 10, wherein determining the configuration further comprises determining a characteristic of an enabled security application enabled.

16. The method of claim 10, wherein applying the restriction further comprises downloading a component to the client device.

17. The method of claim 10, wherein applying the restriction further comprise configuring a virtual sandbox to intercept a communication between the client device and the resource.

18. The method of claim 17, wherein intercepting the communication further comprises blocking a download of at least one file to the client device.

19. The method of claim 10, wherein applying the restriction further comprises:

if the access to the resource is terminated, performing cleanup on the client device including at least one of deleting a cached file, deleting a temporary file, and enabling a disabled system command.

20. The method of claim 10, wherein applying the dynamic policy further comprises determining at least one of a connector, and an adaptor to enable the access to the resource.

21. The method of claim 10, wherein applying the dynamic policy further comprises restricting the access to the resource.

22. A network appliance for managing access to a resource over a network, comprising:

a transceiver for receiving a request for access to the resource from a client device; and

a processor that is configured to perform actions, including:

receiving the request for access;

determining a configuration of the client device;

applying a dynamic policy for the access based, in part, on the determined configuration; and

applying a restriction to the access for the requested resource, wherein the restriction is configured based on the applied dynamic policy.

23. The network appliance of claim 22, wherein the processor is configured to perform further actions, comprising: in response to receiving the request for access to the resource, transmitting a downloadable component to the client device.

24. The network appliance of claim 22, wherein applying the restriction further comprises employing a virtual sandbox that is configured based on the applied dynamic policy.

25. The network appliance of claim 23, wherein determining the configuration of the client device further comprises:

if the client device is configured to receive a downloadable component, providing the downloadable component to the client device.

26. The network appliance of claim 22, wherein applying the dynamic policy further comprises:

if the client device is configured to restricting a download of a component, restricting access to the resource.

27. The network appliance of claim 22, wherein applying the restriction further comprises:

if the client device is configured to restrict a download of a component, intercepting a communication between the client device and the requested resource to perform at least one of preventing an access to file, and restricting an action.

28. A modulated data signal for managing access to a resource over a network, the modulated data signal comprising the actions of:

receiving a request for access to the resource from a client device;

sending a configuration of the client device;

applying a dynamic policy to the access based, in part, on the sent configuration; and

applying a restriction to the access for the requested resource based on the applied dynamic policy.

29. The modulated data signal of claim 28, wherein applying the restriction further comprises configuring a virtual sandbox to intercept a communication between the client device and the resource.

30. The modulated data signal of claim 28, wherein applying the restriction further comprises blocking a download of at least one file to the client device.

31. An apparatus for managing access to a resource over a network, comprising:

a transceiver arranged to receive a request for access to the resource from a client device; and

a policy manager, coupled to the transceiver, that is arranged to perform actions, including:

a means for determining a configuration of the client device;

a means for applying a dynamic policy for the access based, in part, on the determined configuration; and

a means for restricting to the access for the requested resource, wherein the means for restricting is configured based, in part, on the applied dynamic policy.

32. A method for managing access to a resource over a network, comprising:

receiving a request for access to the resource from a client device;

determining a level of security software enabled on the client device;

applying a dynamic policy to the access based, in part, on the determined level of security software enabled; and

applying a restriction to the access for the requested resource based on the applied dynamic policy.

33. A method for managing access to a resource over a network, comprising:

receiving a request for access to the resource from a client device;

determining a configuration of an operating system active on the client device; and

applying a restriction to the access for the requested resource based on the determined configuration of the operating system.

34. A method for managing access to a resource over a network, comprising:

receiving a request for access to the resource from a client device;

determining a presence of a hacker tool active on the client device; and applying a restriction to the access for the requested resource based on the determined presence of the hacker tool.